UNITED STATES DEPARTMENT OF COMMERCE
Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.
08/989,261	12/12/97	PAONE	L 831-2

LM02/0929

CHARLES R HOFFMANN
HOFFMANN & BARON LLP
6900 JERICHO TURNPIKE
SYOSSET NY 11791

EXAMINER	
COMBS, J	
ART UNIT	**PAPER NUMBER**
2767	4

DATE MAILED: 09/29/99

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner of Patents and Trademarks

Office Action Summary

Application No.	Applicant(s)
08/989,261	Luciano F. Paone
Examiner	**Group Art Unit**
Jennifer Coombs	2767

☒ Responsive to communication(s) filed on *Dec 12, 1997* .

☐ This action is **FINAL**.

☐ Since this application is in condition for allowance except for formal matters, **prosecution as to the merits is closed** in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11; 453 O.G. 213.

A shortened statutory period for response to this action is set to expire *3* month(s), or thirty days, whichever is longer, from the mailing date of this communication. Failure to respond within the period for response will cause the application to become abandoned. (35 U.S.C. § 133). Extensions of time may be obtained under the provisions of 37 CFR 1.136(a).

Disposition of Claims

☒ Claim(s) *1-35* is/are pending in the application.

Of the above, claim(s) _____ is/are withdrawn from consideration.

☐ Claim(s) _____ is/are allowed.

☒ Claim(s) *1-35* is/are rejected.

☒ Claim(s) *3 and 15* is/are objected to.

☐ Claims _____ are subject to restriction or election requirement.

Application Papers

☐ See the attached Notice of Draftsperson's Patent Drawing Review, PTO-948.

☐ The drawing(s) filed on _____ is/are objected to by the Examiner.

☐ The proposed drawing correction, filed on _____ is ☐approved ☐disapproved.

☐ The specification is objected to by the Examiner.

☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. § 119

☐ Acknowledgement is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d).

☐ All ☐ Some* ☐ None of the CERTIFIED copies of the priority documents have been

☐ received.

☐ received in Application No. (Series Code/Serial Number) _____ .

☐ received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

*Certified copies not received: _____ .

☐ Acknowledgement is made of a claim for domestic priority under 35 U.S.C. § 119(e).

Attachment(s)

☒ Notice of References Cited, PTO-892

☒ Information Disclosure Statement(s), PTO-1449, Paper No(s). _____

☐ Interview Summary, PTO-413

☐ Notice of Draftsperson's Patent Drawing Review, PTO-948

☐ Notice of Informal Patent Application, PTO-152

--- SEE OFFICE ACTION ON THE FOLLOWING PAGES ---

DETAILED ACTION

Claim Objections

1. Claim 3 is objected to because of the following informalities: "and changes with each data block encrypted" is redundant to "object key is dynamic". Appropriate correction is required.

2. A series of singular dependent claims is permissible in which a dependent claim refers to a preceding claim which, in turn, refers to another preceding claim.

A claim which depends from a dependent claim should not be separated by any claim which does not also depend from said dependent claim. It should be kept in mind that a dependent claim may refer to any preceding independent claim. In general, applicant's sequence will not be changed. See MPEP § 608.01(n).

As per claim 15, the dependence is based on claim 17. Please make appropriate corrections.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are

such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 9, 12, 17-20, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ronald L. Rivest (U.S. Patent # 5,724,428) in view of M. Greg Shanton (U.S. Patent # 5,369,702).

As per claims 1-2, 9, 12, 17-20, and 22, Rivest fails to teach a computer implemented method for encrypting data wherein creating an object key comprising data and methods that operate on said. However Shanton clearly suggests creating an object key comprising data and methods that operate on said data (col. 3, lines 35-68 and col.4, lines 1-34). As both Rivest and Shanton disclose their encryption systems it would have been obvious to a skilled person in the art at the time of the invention to incorporate creating an object key comprising data and methods that operate on said data because it allows for randomness in the encryption/decryption process.

5. Claims 3-8, 11, 13, 14, 16, 29, 31-32, and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest in view of Shanton in further view of Alfred J. Menezes et al. (Handbook of Applied Cryptography).

As per claims 3-8, 11, 13, 14, 16, 29, and 31-32, Rivest in view of Shanton fails to teach a computer implemented method wherein the object key is dynamic for each encrypted data block; modifying the object key based on seeding from the random session object key before

each input data block so that each block is encrypted based on different object key; associated with a different key schedule for encrypting each data block with said different key schedule; and creating initial state of the random session key object using a time clock. However, Menezes teaches a computer implemented method wherein the object key is dynamic for each encrypted data block (pg. 490-491); modifying the object key based on seeding from the random session object key before each input data block so that each block is encrypted based on different object key (pg. 20-21, 170); associated with a different key schedule for encrypting each data block with said different key schedule (pg. 255-256); and creating initial state of the random session key object using a time clock (pg. 398-399). As Rivest in view of Shanton in further view of Menezes disclose their encryption systems it would have been obvious to a skilled person in the art at the time of the invention to incorporate a computer implemented method wherein the object key is dynamic for each encrypted data block; modifying the object key based on seeding from the random session object key before each input data block so that each block is encrypted based on different object key; associated with a different key schedule for encrypting each data block with said different key schedule; and creating initial state of the random session key object using a time clock because it allows for randomness in the encryption/decryption process.

As per claim 34, Rivest in view of Shanton fails to teach a computer implemented method wherein the block cipher encryption/decryption process includes use of a keyed transposition of a sequence of integers provides a coat of substitution rounds for a particular input entering an S-box. However, Menezes teaches a computer implemented method wherein

the block cipher encryption/decryption process includes use of a keyed transposition of a sequence of integers provides a coat of substitution rounds for a particular input entering an S-box (pg.252). As Rivest in view of Shanton in further view of Menezes disclose their encryption systems it would have been obvious to a skilled person in the art at the time of the invention to incorporate a computer implemented method wherein the block cipher encryption/decryption process includes use of a keyed transposition of a sequence of integers provides a coat of substitution rounds for a particular input entering an S-box because it allows for randomness in the encryption/decryption process.

As per claims 25-28, 33, and 35, Rivest in view of Shanton fails to teach a computer method for authenticating cipher text, wherein generating digital signature of a user using the cipher text as input into a keyed one-way hash function; appending the digital signature to the input ciphertext; and modifying the running message digest using a bit-wise exclusive or to the next input data block. However, Menezes teaches a computer method for authenticating cipher text, wherein generating digital signature of a user using the cipher text as input into a keyed one-way hash function (pg. 325); appending the digital signature to the input ciphertext (pg. 426-429); and modifying the running message digest using a bit-wise exclusive or to the next input data block (pg.321-322). As Rivest in view of Shanton in further view of Menezes disclose their encryption systems it would have been obvious to a skilled person in the art at the time of the invention to incorporate a computer method for authenticating cipher text, wherein generating digital signature of a user using the cipher text as input into a keyed one-way hash

function; appending the digital signature to the input ciphertext; and modifying the running message digest using a bit-wise exclusive or to the next input data block because it allows for increased security of the message.

6. Claims 10, 15, 21, 23-24, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rivest in view of Shanton in further view of well known art.

As per claims 10, 15, and 24, Rivest in view of Shanton fail to teach a computer implemented method wherein said object key is dynamic and modification method of said object key includes a hashing function. Official Notice is taken that both the concept and the advantages of a computer implemented method wherein said object key is dynamic and modification method of said object key includes a hashing function is well known and expected in the art. It would have been obvious to include a computer implemented method wherein said object key is dynamic and modification method of said object key includes a hashing function because it allows for randomness in the encryption/decryption process.

As per claim 21, Rivest in view of Shanton fail to teach a computer implemented method wherein the block cipher encrypting process groups the ciphertext in a 32-bit sliding window. Official Notice is taken that both the concept and the advantages of a computer implemented method wherein the block cipher encrypting process groups the ciphertext in a 32-bit sliding window is well known and expected in the art. It would have been obvious to include a

computer implemented method wherein the block cipher encrypting process groups the ciphertext in a 32-bit sliding window because it allows for ease in the processing the data.

As per claim 23, Rivest in view of Shanton fail to teach a computer implemented method wherein the last transpostioning step uses a switch key. Official Notice is taken that both the concept and the advantages of a computer implemented method wherein the last transpostioning step uses a switch key is well known and expected in the art. It would have been obvious to include a computer implemented method wherein the last transpostioning step uses a switch key because it allows for data to be routed.

As per claim 30, Rivest in view of Shanton fail to teach a cryptographic communications system comprising each computer system including a central processing unit and a memory storage device for executing a block cipher encryption/decryption process. Official Notice is taken that both the concept and the advantages of a cryptographic communications system comprising each computer system including a central processing unit and a memory storage device for executing a block cipher encryption/decryption process is well known and expected in the art. It would have been obvious to include a cryptographic communications system comprising each computer system including a central processing unit and a memory storage device for executing a block cipher encryption/decryption process because it allows for the computing and processing methods to occur.

Conclusion

7. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Any inquiry concerning this communication from the examiner should be directed to Jennifer Coombs whose telephone number is (703) 306-5540 . The examiner can normally be reached Monday-Thursday from 7:00 A.M. to 5:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tod Swann, can be reached at (703) 308-7791.

The fax number for Formal or Official faxes to Technology Center 2700 is (703) 308-9051 or 9052. Draft or Informal faxes for this Art Unit can be submitted to (703) 305-0040.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 305-3900.

TOD R. SWANN
SUPERVISORY PATENT EXAMINER
GROUP 2700

jc

September 25, 1999